Testimony of

Stephen J. Rohleder
Managing Partner, USA Government Market Unit

Accenture

Securing our Nation's Infrastructure

Before

Subcommittee on Science, Technology and Space
Senate Committee on Commerce, Science and Transportation

December 5, 2001

Introduction

Chairman Wyden, Senator Allen, Members of the Subcommittee, I am Stephen J. Rohleder, the managing partner of the USA Government Market Unit of Accenture. I appreciate the opportunity to testify before you today.

Accenture's expertise is in the areas of technology and business. We employ more than 75,000 people in 46 countries who serve clients across all industries – telecommunications, electronics, high technology, financial services, resources, products, and federal, state and local governments. We serve 86 of the Fortune 100.

As part of the normal course of business, we conducted an assessment of the situations faced by our clients, the impact on their industries, and how they should meet the opportunities and challenges ahead. I will share some of these findings and suggestions today. I will also comment on the idea of establishing a NetGuard to respond to future terrorists attacks.

Ground Zero

On September 11th, Accenture, along with the rest of the civilized world, watched in horror as the tragic results of unprecedented terrorism unfolded in New York, in Pennsylvania and in our nation's Capital. Our employees, our clients, our families and friends have all been directly touched by the devastation. We, like so many New Yorkers, were also called to serve in a government-private partnership to help the city in a time of crisis.

In the days following the terrorist attacks on the World Trade Center, Mayor Guiliani's Office asked Accenture to manage the establishment of a new

Family Assistance Center. More than 130 Accenture people, along with some of their families, worked with the Office of Emergency Management, the New York Police Department, the Medical Examiner, the Red Cross, the Mayor's office and other private companies to create the new center, which enables people to gain information about loved ones, as well as to leave information about the people they are seeking, request a death certificate or apply for financial assistance.

In less than 72 hours, Accenture employees spearheaded the transformation of a barren warehouse located on Pier 94 in Manhattan to a fully functioning facility, installing 130,000-square feet of carpet, over 250 workstations, a network supporting more than 250 personal computers and 500 phones and free Internet access. The Center has served as the primary resource facility for relatives and friends of those missing since the disaster. Since the facility opened, there have been more than 60,000 family visits. The families who utilize the services of the Center include not only those who lost loved ones, but also those who lost their jobs or homes as a result of the disaster. Once operational, Accenture built applications to facilitate processes that helped people, including tracking the status of applications for death certifications, distribution of memorial urns, and analyzing information regarding the number of missing persons.

There are a number of important lessons learned from the establishment of the Family Center.

- Governments must be able to establish crisis management centers rapidly to meet unexpected large-scale human disaster.
- They need to utilize information technology and customer relationship management techniques to ensure that citizens are served rapidly and

easily.

- Victims of disaster or terrorism should be able to access the assistance of the government with the least amount of trauma – one-stop assistance should be the goal.
- Governments need to team with the private sector to provide services using best commercial business processes and technology.
- Over time, virtual assistance can, and should be provided to families on an on-going basis.

America on Notice

Today, the markets have rebounded to the levels they were in early September. And the good news is that market indicators point to further gains in 2002. The terrorist attacks on America have failed to achieve their financial objectives, but we *have* been put on notice. We have learned that war can now be waged on our shores, and our infrastructures are tempting targets.

The attacks on the World Trade Center were in many ways a wake up call – vivid illustration of the centrality of our information infrastructure and its value in times of threat – to government, to business and to individuals. Cell phone calls from stricken United Airlines flight 93 over Pennsylvania seem to have played a role in preventing the terrorists from reaching their intended target. Wireless email messages from World Trade Center brought family members together and sometimes grief. Internet messages got through when traditional phone networks strained under the load of record call volumes.

Unfortunately, the value and vulnerability of our nation's information infrastructure has not gone unnoticed by those terrorists who would target the United States. The proliferation of the Internet and the increased

integration of our nation's infrastructures create the opportunity for a new form of asymmetrical threat. Many government and private sector computer systems are interconnected through the Internet, a network originally designed to support robust network interconnection, not high security.[1] The original Defense Advanced Research Agency (DARPA) design has worked remarkably well, with over 400 million users now online worldwide.[2] New technology developments including Internet-enabled cell phones, wireless email and mobile commerce are expected to expand Internet usage exponentially. And yet as Internet usage increases, the likelihood and impact of cyber terrorism goes up concomitantly – unless we take actions now to appropriately secure the infrastructure for public and private sector use.

The President's appointment of Pennsylvania Governor Tom Ridge to head up the Office of Homeland Defense sets the stage for unprecedented cooperation and coordination between the private sector and government to tackle these cyber security weaknesses. It also can serve as "home" for innovative ways for intergovernmental and public-private information sharing to defend against any new terrorist attacks.

In fact, the United States and many of our allies present a wide array of potential targets beyond military systems. These include: the air traffic control system, banking and capital markets, telecommunications systems, power supplies, water resources, and oil and gas delivery systems. Let's look back, and then look forward.

---

[1] David D. Clark, "The Design Philosophy of the DARPA Internet Protocols," Proc. SIGCOMM '88, Computer Communication Review Vol. 18, No. 4, August 1988, pp. 106–114)

[2] *CIA World Factbook 2001*

The Aftermath

In the aftermath of September 11, our clients faced a number of challenges. We need to learn from this, and certainly leading executives and organizations must be prepared for business continuity along the following five areas.

1) Initiate Immediate Recovery – Most large companies had effective disaster recovery programs for major software systems. But data located in departmental "local area networks," many of which perform very important business functions, was lost. Many did not figure on losing facilities. Many small and medium enterprises had greater challenges, often unable to afford or focus on business continuity planning. Government, including Congress, faced challenges being on-line and connected to its constituents when buildings were evacuated, highlighting the need for a "virtual" government planning.

2) Establish Temporary Operations - Companies scrambled to secure temporary working facilities in hotels, or through telecommuting from home or other offices, but business communications capabilities continue to be limited because so much of lower Manhattan's phone system was concentrated in hubs that were located in or near the World Trade Center. Despite remarkable efforts by the phone companies involved, lines are often inadequate, access to voicemail and email – required business tools for many – remains severely limited.

3) Determine Permanent Operating Facilities - Companies are evaluating the wisdom of geographically concentrated staffs as they make plans to secure permanent facilities. Some are dispersing employees in the local area or

beyond. These shifts in worker locations are causing aftershocks in areas ranging from city planning to suburban telephone systems.

4) Embrace the Virtual Workplace - Organizations can reduce the risk of terrorist attacks by employing information technologies that enable "virtual" workplaces. Examples include: instant messaging, electronic mail, groupware and web conferencing, some of the most reliable technologies during and immediately after the attack

5) Preparing for Ensuing Economic Impacts – Many companies immediately understood what this "demand shock" meant to them – and they moved to reduce their costs accordingly. A few businesses are thriving. For others, it will take months or even years for the full impact to be understood. "Supply" must be adjusted accordingly.

These are basic elements of business continuity planning. Most business and government continuity plans we have seen didn't seriously consider the types of threats that have become familiar in the past two months. Businesses and Government need a new kind of planning for the future. We believe there is a strong role for the Office of Homeland Security to play in helping coordinate federal, state, local and private sector coordinated continuity planning.

Looking Forward for Business and Government Planning

As business and organization leaders, we are all trying to grapple with a great deal of uncertainty. What then lies ahead for business and government in this new era? Will fears of terrorism lock the economy in a death spiral, or will fiscal and monetary policy result in a soft landing and quick recovery?

We must be better prepared for attacks on our soil, we must integrate greater security in what we do, and we must work together as public and private sectors. As business leaders, we are challenged to do what we have done so well in the past: marshal technology and our creative genius to continue to drive better business and society towards a successful future. Government, too, must heed this wake-up call, and move promptly to protect its information systems. Beyond the need we have discussed to have business continuity planning that recognizes today's threats, there are several things we must do:

Invest in Innovation for Global Competitiveness

At a time when terrorists would want us to retreat, we need to recognize where we are in the current business and technology cycles. We are seeing business trends like outsourcing creating efficiency and an improvement in global standards of living. We are seeing the "industrialization" of systems development – using labor arbitrage and new technologies to improve cost efficiency and productivity. In fact, despite the spectacular decline of technology markets recently, technology is poised for a rebound. Every important digital technology over the past 50 years has seen a boom followed by a major shakeout that lasted typically four to eight quarters. After the shakeout, the surviving competitors enjoyed marked growth, as much as 100-fold. New high-speed Internet-ready computers, broadband networks, wireless devices and, most importantly, software that enables dynamic inter-business commerce, will power new approaches to commerce while fueling the next market advance. Government and business leaders must have the courage to drive investment. Policymakers must take advantage of bipartisan times. Businesses could take advantage of historically low interest rates to deploy new innovation for stronger global competitiveness

tomorrow. We must invest for the future.

Leverage Technology to Achieve Security without Sacrificing Productivity

Conventional wisdom is that increased security costs more without any benefits. When we think in traditional terms – hiring high quality security guards, increased monitoring, etc, that is certainly true. On the other hand, investments in security-related technology often bring many side benefits that lead to greater productivity. A new operating system is more secure, but also has many more features to be exploited. In many organizations, over 90 percent of the operational information is still in paper form. Investment in digital content management systems can replace paper with their digital equivalents so information can be safely distributed and easily reproduced. But at the same time digital content can be used for new, more efficient approaches to training. Certainly the Federal Government could serve as a model, streamlining paper-heavy processes, while utilizing technology to tackle some of its most pressing homeland security training needs.

Investment in a high quality, secured network could allow greater collaboration with reduced travel. Advances in networking hardware and software enable us to achieve new levels of inter-enterprise integration that further secure while streamlining transactions with trading partners. Investment will also provide the added benefit of network redundancy.

Mobile wireless devices and advanced security techniques can create safe, virtual workplaces for our people. This technology exists today. The right investments in technology for security's sake could in fact stimulate key sectors of our economy. As policymakers, for example, you should consider

using tax incentives like accelerated depreciation of technology equipment to stimulate such investments.

Technology can be used to protect people as well as networks. For example, in the area of airline security, Accenture recently conducted a study that found six of 10 airline travelers who have canceled their upcoming holiday flights are doing so because of security concerns and the likelihood of long lines. Technology can help improve security long before passengers reach the airport, increasing passenger confidence and ease of travel.

Build Public/Private Partnerships to Further a Secure Commerce Infrastructure

While we will face challenges in the short-term, economic and technological indicators point to recovery next year. Among the many opportunities we see, one stands out: the secure, broadband digital commerce infrastructure. Technology companies have worked to establish portions of this infrastructure, but the job remains unfinished. Today, the right public-private partnership can help create secure information infrastructure that will be the backbone of tomorrow's economy. Mechanisms to stimulate deployment including regulation, tax incentives, and government funding, should be considered.

Congress should examine existing emergency response processes already in place through the Federal Emergency Management System and state and local authorities. While industry can dedicate volunteer resources, knowledge capital and skills, industry efforts should complement federal emergency management efforts to organize and provide infrastructure. Partnerships should be created at the Federal, state and local level.

Clearly, there is a need for the public and private sectors to carefully plan for the most efficient and effective response to terrorist attacks. When the city of New York asked Accenture for help, we were able to respond without haste because of the capabilities, resources, and dedication of our employees. The response was not limited to network-building and technology, but implementing industry best practices and coordination among agencies. There are a number of areas where Government can help facilitate public-private partnerships.

NetGuard

The concept of a NetGuard is an interesting one that should be examined further. Developing a trained and technology-able corps of volunteers to support information technology restoration could be beneficial to government, the community and business. Clearly the details need to be fleshed out. NetGuard may have some practical problems in implementation. The following are four recommendations for the Committee's consideration:

1) Protection of proprietary data and technology will be a major issue for businesses. NetGuard volunteers would likely be drawn from across industry and from competing companies. There would need to be safeguards put in place to provide protection for proprietary assets accessed by NetGuard volunteers.

2) A major challenge for the deployment of a NetGuard would be matching skills with need. For example, a project manager might not have the technical skills to restore the various software and equipment elements of

telecommunications networks. A process would need to be developed to effectively match technology skills to need in times of crisis. In addition, a protocol would need to be developed to determine how NetGuard volunteers would be deployed. Government should consult closely with the private sector on these plans to ensure fairness.

3) Companies will need to plan for and assess the impact of losing key personnel for an extended period of time during a crisis. There may also need to be exemptions provided for personnel in companies that are directly impacted by a crisis who may be NetGuard volunteers.

4) Training of a NetGuard force would need to be dynamic to keep up with technology and allow for flexibility since volunteers will likely be located across the United States. Accenture is working with a number of clients to migrate more "on-site" classroom training to web-based training in a "virtual" classroom. Given the rapid changes in the industry, web-based training could allow for rapid deliver of training material while also reducing costs.

Digital Tech Corps

Accenture strongly supports public-private partnerships. In response to September 11th, Accenture offered a manager to become a fellow at the Department of Commerce. This fellow is assisting small to medium-sized businesses get back on their feet.

Earlier this year, Accenture supported legislation introduced by Congressman Tom Davis that would establish a Digital Tech Corps. H.R. 2678, the Digital Tech Corps Act would provide for the exchange of

government and industry IT professionals for up to two years. While we supported the concept to help ease the shortage of IT workers in the Federal Government and to spur cross-pollination of best practices, we believe it could also serve as an opportunity for public and private sector IT professionals to share best practices for emergency IT responses.

Office of Homeland Security

We also believe that the Office of Homeland Security should play an integral role in helping the public and private sector provide continuity and disaster planning for their communities while coordinating an effective and coordinated response in times of crisis. Information technology should be utilized to facilitate more effective communication and coordination between all appropriate law enforcement agencies in a secure, real-time fashion. We believe that by utilizing commercial technology, some of the challenges of interagency and intergovernmental agency communication and cooperation could be diminished significantly.

Conclusion: Make this our Finest Hour

The terrorists sought to undermine our businesses and to destroy the "American way" with fear. As business and government leaders, we can stand united to take the best we have to offer to secure this nation's infrastructure and to take this opportunity to lead with innovation. Years from now, as we look back upon this time, let history show that we did not give in, and that the tragedies of September 2001 spurred us all to our finest hour.

Mr. Chairman, thank you for inviting me to appear before the Subcommittee. Accenture is committed to working with you as you further develop the

NetGuard proposal.